A New Multicarrier/ Signature Iterative Generalized Least-Squares (M-IGLS) For Hidden Valuable Data from Digital Media

Henry Arun Steven [#1], Pentapati Aditya [#2] , Bulusu Vagdevi Abhigna [#3] , Puvvala Nandini[#4], Mr.B.A.Swamy [*5]

[#1]B.Tech Student, [#2] B.Tech Student, [#3] B.Tech Student, [#4] B.Tech Student, [*5] Assistant Professor

Department of Information Technology,
Lendi Institute of Engineering and Technology College,
Jonnada, Denkada Mandalam, Vizianagaram Dist, AP, India.

Abstract

We consider stegnography as a new mode of providing security for secret communication. By using this new mechanism a lot of users are sending most valuable messages or data files in a secure manner over various public channels, so that a third party attacker cant able to detect the presence of secret message present inside the received data. The process of hiding valuable secret message inside a master or dummy file mechanism is known as embedding, and the reverse process of extracting the hidden data from the dummy file or master file is known as de-embedding. In this paper, we mainly consider the problem of de-embedding blindly data embedded over a wide band in a spectrum domain of a digital medium like image, audio and video. We proposed a new multicarrier/ signature iterative generalized least-squares (M-IGLS) core method to seek unknown data hidden in hosts via multicarrier spread-spectrum embedding technique. Our experimental results clearly tell that the proposed work can able to achieve very high level of security in hiding valuable data inside a digital data.

Keywords

Blind Detection, Covert Communications, Data Hiding, Information Hiding, Spread-Spectrum Embedding, Stegnography, Watermarking.

1. Introduction

Now a day's communication of digital data (Image, Video, and Audio) through public channels have become a most critical problem in society. For transmitting of valuable sensitive information or hidden messages over the internet is always a big issue .The data even though having no security while transmitting through public channels it is still getting a lot of problems for several user's. Data Embedding is a mechanism of hiding valuable data or text files inside a master file or dummy file is called as data embedding method. We have some annotation based mechanisms, where secondary data are mainly stored secretly into digital multimedia content[1] either any of the 3 types of digital data like Image,Audio,Video to give a more security during delivery of information for various useful purposes. We also know that Fragile watermarking technique may also be intended especially to detect future tampering of data, hidden invisible low probability content to be hide within the digital media with an highest form of validation and security for tracing purposes [2][3][4].

Steganography is a branch which mainly deals with Embedding and De-Embedding of original content within a Cover file like image, video, or audio for giving highest form of security for that data, which is also known as "covered writing method" in Greek literature. This technique is mainly used for establishing relation between more than two persons in a very secured manner without releasing or misusing any small part of embedded data [5],[6],[7],[8],[9].

There are mainly four important metrics for giving data security with the help of watermarking technique. They are as foll**ows** [10]:

1. Payload Metric

This is one of the main important metric which is especially used for finding the delivery rate of the information which is send. With the help of this metric only the user is able to measure the delivery rate for the data embedded with in Cover data.

2. Robustness Metric

This is another metric which is used in stegnography method, where it is mainly used for finding the resistance to noise/disturbance from the hidden data.

3. Transparency Metric

This is the third metric which is also available in stegnography method, where this is used for measuring a very low Cover Image distortion especially used to measure in concealment purposes.

4. Security Metric

This is the final metric that is used in the process of stegnography, where this is mainly used for measuring the inability of the unauthorized users who want to break or de-embedded the data over communication channel.

We can clearly find the advantages of stegnography mechanism from the figure .1, which clearly states the explanation of stegnography method used for embedding an image within an image, the same principle is used for embedding audio and video also within same type of formats or different type of formats like audio in image, image in audio, video in image, image in video, image in image, video in video, audio in audio and so on.

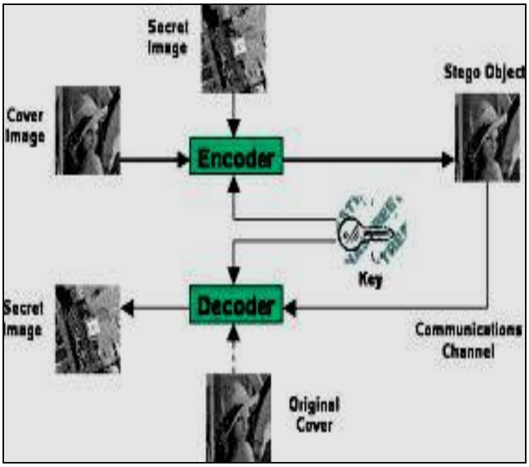


Fig. 1. Block diagram of Stegnography Mechanism

In this paper, we mainly develop a new (M-IGLS) steganalysis algorithm for storing the valuable hidden data and also extracting the valuable hidden data from the cover data.We also propose a new algorithmic upgrade for this paper which is referred to as cross-correlation enhanced M-IGLS (CC-M-IGLS). This new enhanced principle relies mainly on analyzing independent M-IGLS executions on the Cover data and several experimental studies clearly state that this mechanism is able to achieve hidden data recovery with highest probability.

The following notations are used throughout the whole published paper.

- **Carrier File**

  A file is said to be carrier file which has hidden information inside of it. This is also known as Cover file.

- **Steganalysis**

  It is defined as the process of detecting valuable hidden information within a cover file.

- **Stego-Medium**

  It is mainly used to represent the

medium in which the information is hidden.

- **Redundant Bits**

It is used to represent pieces of information inside a file which can be overwritten or altered without damaging the file.

- **LSB (Least Significant Bytes)**

This is mainly used to represent the bytes which are not used or at least aren't that important in file embedding

- **Embed**

The process of hiding digital data or text data inside any of the digital form of sources like Audio/Video/Image.

- **Extract**

Extract is the process of detecting or finding the hidden form of digital data in any of the cover data file.

- **AU Format**

AU is one of the most common audio formats used on the Web. It was created by Sun Microsystems and is sometimes referred to as "audio/basic" format. Most browsers support the au format with their internal sound players. An au-formatted file has this extension: sound.au

Along with the above notations and terminologies we also use the following notations in the entire paper, they are as follows:

Boldface lower-case letters in this paper indicate column vectors and bold face upper-case letters in this paper indicate matrices. Where Capital Letter R denotes the set of all real numbers; $(\cdot)^T$ denotes Transpose Matrix; Tr $\{\cdot\}$ is known as trace of matrix; I_L is the L × L identity matrix; sgn $\{\cdot\}$ denotes zero-threshold quantization; and E $\{\cdot\}$ represents statistical expectation. Finally, $|\cdot|$, $\|\cdot\|$, and $\|\cdot\|_F$ are the scalar magnitude, vector norm, and matrix Frobenius norm, respectively.

2. MCSS Embedding and Extraction Technique

MCSS is also known as multi-carrier stegnography signature.

Let us consider a cover image represented as

$H \in M^{N1\times N2}$

Where M denotes the finite state of image and

$N_1 \times N_2$ is also represented as matrix form of representing image size in the form of pixels.

Initially the image H is divided into M different local non-overlapping blocks of varying size N_1N_2/M.

Each divided block namely, H1, H2, ...,H_M, is to carry K hidden information bits (KM bits total image payload) which is performed mainly on 2-Dimensional data also known as T.

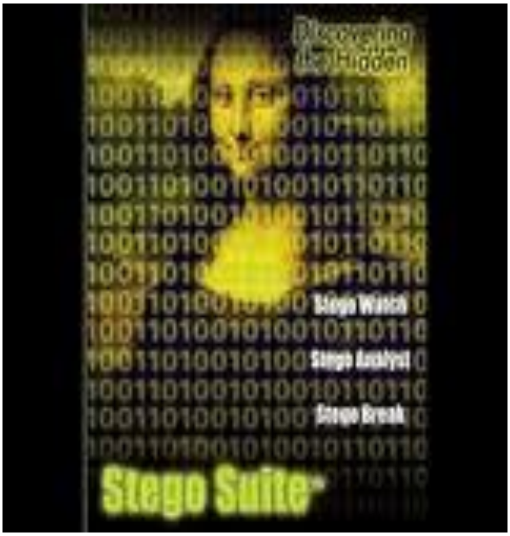


Fig. 2. (a) Stegno Image

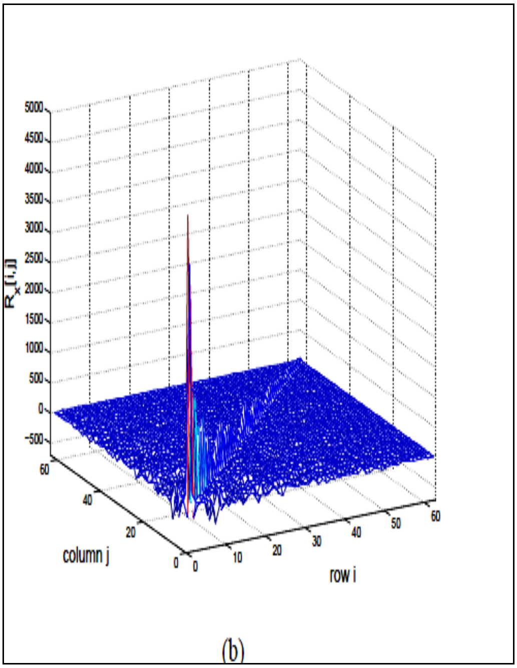


Fig. 2. (a) Represents Stegno image example H= {0, 1, 255}256×256. (b) Host data autocorrelation matrix (8 × 8 DCT, 63-bin host).

For our development we mainly require the auto correlation matrix which is finally formed by the Cover Data. For example, we take 8×8 DCT with 63-bin Cover data formation (excluding only the dc coefficient) for the 256×256 gray-scale Stegno image in Fig. 2(a) gives the host autocorrelation matrix Rx in Fig. 2(b) [11].

2.1 MCSS Embedding Technique

We consider initially K distinct message bit sequences, {$b_k(1)$, $b_k(2)$, . . . , $b_k(M)$}, k = 1, 2, . . . ,K, $b_k(m)$ ∈ {•≠_1}, m = 1, . . . ,M, each of varying length M bits. The K message sequences may be to be delivered to K distinct corresponding recipients or they are just K portions of one large message sequence to be transmitted to one recipient. In particular, the mth bit from each of the K sequences, $b_1(m)$, . . . , $b_K(m)$, is simultaneously hidden in the mth transform-domain host vector x(m) via additive SS embedding by means of K spreading sequences (carriers) $s_k \in R^L$, $\|s_k\| = 1$, k = 1, 2, . . . ,K,

$$\mathbf{y}(m) = \sum_{k=1}^{n} A_k b_k(m)\mathbf{s}_k + \mathbf{x}(m) + \mathbf{n}(m),\ m = 1, 2, \ldots, M, \quad (1)$$

Where b_k the contribution that is required for every individual embedded message bit to the composite signal which is defined as $A_k b_k s_k$

Here in the equation 2 we clearly denote the block mean-squared distortion to the original Cover data x due to the embedded k message alone as follows

$$\mathcal{D}_k = \mathbb{E}\{\|A_k \mathbf{s}_k b_k\|^2\} = A_k^2,\ k = 1, 2, \ldots, K. \quad (2)$$

Once after the equation(2) is obtained, we finally undergo statistical independence of hidden messages, the block mean squared distortion of the original image due to the total, multimessage, insertion of data is defined as follows

$$\mathcal{D} = \sum_{k=1}^{K} A_k^2.$$

Once the statistical independence is observed we finally find the intend recipient of the kth message with knowledge of the kth carrier s_k can perform embedded bit recovery by looking at the sign of the output of the minimum-mean-square error (MMSE) filter $w_{MMSE,k} = R^{-1}{}_{y}\, s_k$.

$$\hat{b}_k(m) = \mathrm{sgn}\{\mathbf{w}_{MMSE,k}^T \mathbf{y}(m)\} = \mathrm{sgn}\{\mathbf{s}_k^T \mathbf{R}_y^{-1} \mathbf{y}(m)\} \quad (3)$$

Where Ry is defined as the autocorrelation matrix of the host-plus-data plus- noise vectors

$$\mathbf{R}_y \triangleq \mathbb{E}\{\mathbf{y}\mathbf{y}^T\} = \mathbf{R}_x + \sum_{k=1}^{K} A_k^2 \mathbf{s}_k \mathbf{s}_k^T + \sigma_n^2 \mathbf{I}_L. \quad (4)$$

3. Project Implementation Modules

Implementation of a project is the stage where the theoretical design is completely turned out into a working system. Thus it can be considered to be the most critical stage in achieving a successful new system and in giving the user, confidence that the new system will work and be effective. As our application is implemented in Java as the chosen technology with Java Swings as front end user interfaces. Here we are also using Remote Method Invocation method in java to start the invocation of sender and receiver nodes. The following paper is divided into following four modules. They are as follows:

1. Digital Steganography Module.
2. Multi-Carrier Spread Spectrum Embedding.
3. Image Encryption and Embedding Module.
4. Image decryption and De-Embedding Module.

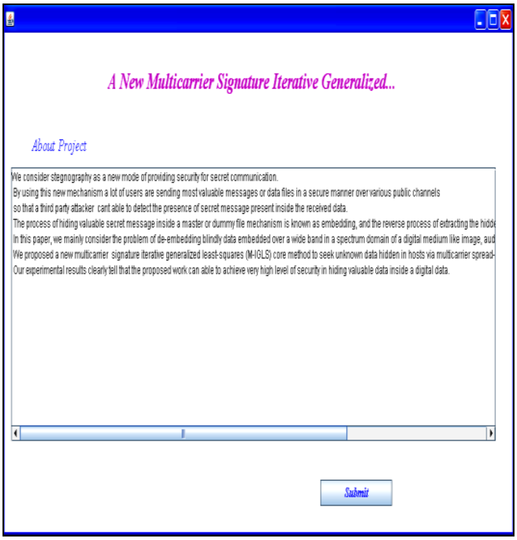
With the help of these four modules we are able to provide security for the hidden data over transmission channel.

4. Experimental Results

In this paper, we have mainly sender who want to embed the valuable hidden data onto a cover page and wants to transmit over communication channel, for this the window we created in java looks like below

The below window is the starting window or home window for our proposed project. In this window we will tell the project abstract in detail in the text area that is present in that main window. If the user who wishes to participate in stegnography process, he should click on submit button so that he can be enter into the home page, if not he will not be directed to stegnography page.

Main Window



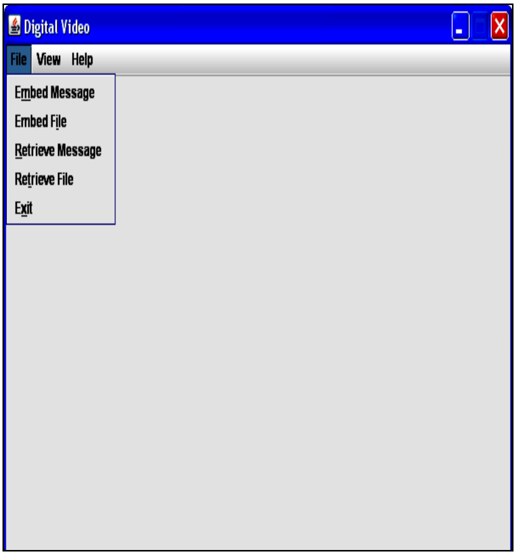
A New Multicarrier Signature Iterative Generalized...

About Project

We consider stegnography as a new mode of providing security for secret communication.
By using this new mechanism a lot of users are sending most valuable messages or data files in a secure manner over various public channels
so that a third party attacker cant able to detect the presence of secret message present inside the received data.
The process of hiding valuable secret message inside a master or dummy file mechanism is known as embedding, and the reverse process of extracting the hidde
In this paper, we mainly consider the problem of de-embedding blindly data embedded over a wide band in a spectrum domain of a digital medium like image, aud
We proposed a new multicarrier signature iterative generalized least-squares (M-IGLS) core method to seek unknown data hidden in hosts via multicarrier spread-
Our experimental results clearly tell that the proposed work can able to achieve very high level of security in hiding valuable data inside a digital data.

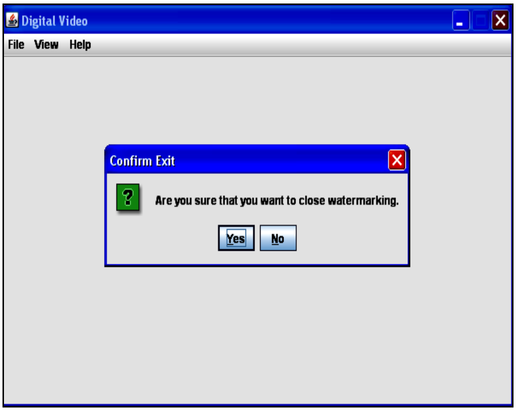
Once after we click on submit button the following Stegnography window will displays in which we have facility of embedding message, embedding a file.

Stegnography Window



Exit Window

This window is mainly designed in order to ask confirmation whenever any user who wish to close the current process.If the user clicks on yes option then window gets closed otherwise it will be in same stegnography window.



Are you sure that you want to close watermarking.

5. Conclusion

In this paper, we mainly targeted on the problem of hiding sensitive valuable information into any digital form of data like audio, video, image.And also how to extract the hidden data from the cover node, for this problem we have used multi-carrier/signature spread-spectrum embedding. Neither the original host nor the embedding carriers are assumed to be available. We also developed a new mechanism of low complexity multi-carrier iterative generalized least-squares (M-IGLS) core algorithm. Our experimental work tells that our proposed methods can achieve high probability of error rather than other methods.

6. References

[1] F. A. P. Petitcolas, R. J. Anderson, and M. G. Kuhn, “Information hiding: A survey,” *Proc. IEEE (Special Issue on Identification and Protection of Multimedia Information)*, vol. 87, pp. 1062-1078, July 1999.

[2] I. J. Cox, M. L. Miller, and J. A. Bloom, *Digital Watermarking*. San Francisco, CA: Morgan-Kaufmann, 2002.

[3] F. Hartung and M. Kutter, “Multimedia watermarking techniques,” *Proc. IEEE (Special Issue on Identification and Protection of Multimedia Information)*, vol. 87, pp. 1079-1107, July 1999.

[4] G. C. Langelaar, I. Setyawan, and R. L. Lagendijk, “Watermarking digital image and video data: A state-of-the-art overview,” *IEEE Signal Processing Magazine*, vol. 17, pp. 20-46, Sept. 2000.

[5] N. F. Johnson and S. Katzenbeisser, “A survey of steganographic techniques,” in *Information Hiding*, S. Katzenbeisser and F. Petitcolas Eds. Norwood, MA: Artech House, 2000, pp. 43-78.

[6] S. Wang and H. Wang, “Cyber warfare: Steganography vs. steganalysis,” *Communications of the ACM*, vol. 47, pp. 76-82, Oct. 2004.

[7] C. Cachin, “An information-theoretic model for steganography,” in *Proc. 2nd Intern. Workshop on Information Hiding*, Portland, OR, Apr. 1998, pp. 306-318.

[8] G. J. Simmons, “The prisoner’s problem and the subliminal channel,” in *Advances in Cryptology: Proc. CRYPTO’83*. New York, NY: Plenum, 1984, pp. 51-67.

[9] J. Fridrich, *Steganography in Digital Media, Principles, Algorithms, and Applications*. Combridge, UK: Combridge Univeristy Press, 2010.

[10] Y. Wang and P. Moulin, “Perfectly secure steganography: Capacity, error exponents, and code constructions,” *IEEE Trans. Inform. Theory*, vol. 54, pp. 2706-2722, June 2008.

[11] M. Gkizeli, D. A. Pados, and M. J. Medley, “Optimal signature design for spread-spectrum steganography,” *IEEE Trans. Image Proc.*, vol. 16, pp. 391-405, Feb. 2007.

7. About the Authors

Henry Arun Steven is currently pursuing his B.Tech in Dept of Information & Technology, Lendi Institute of Engineering and Technology College, Jonnada, Denkada Mandalam, Vizianagaram Dist. His area of interests includes DBMS, Java Programming Technology.

Pentapati Aditya is currently pursuing his B.Tech in Dept of Information & Technology, Lendi Institute of Engineering and Technology College, Jonnada, Denkada Mandalam, Vizianagaram Dist. His area of interests includes DBMS, Java Programming Technology, Android and Dot net.

Bulusu Vagdevi Abhigna is currently pursuing her B.Tech in Dept of Information & Technology, Lendi Institute of Engineering and Technology College, Jonnada, Denkada Mandalam, Vizianagaram Dist. Her area of interests includes DBMS, Java Programming Technology and Android.

Puvvala Nandini is currently pursuing her B.Tech in Dept of Information & Technology, Lendi Institute of Engineering and Technology College, Jonnada, Denkada Mandalam, Vizianagaram Dist. Her area of interests includes Cryptographic Network Systems.

Mr.B.A.Swamy received his M.Tech degree in Computer Science & Engineering from GMRIT Rajam, A.P, India and B.Tech degree in Computer Science & Engineering from TPIST Bobbili, India. Currently he is working as an Assistant Professor in Dept of Computer Science & Engineering, Lendi Institute of Engineering and Technology College, Jonnada, Denkada Mandalam, Vizianagaram Dist.His research interests include Networks, Manets and Operating Systems.